Where do I get a certificate?	There are three DOD approved resources for the ECA: http://www.identrust.com/index.html https://www.verisign.com/authentication/government-authentication/DOD-interoperability/index.html http://www.eca.orc.com/index.html
What is the cost?	Cost ranges from $120 to $135
How long are they good for?	One Year
How many do I need for my company?	One per person who requires access to a DOD system.
What if personnel travel? Will the cert be good?	Yes the cert can be copied to a thumb drive, or to another location
Who can answer questions?	Questions regarding the cert, call the company in which purchase was made. Questions on syncing up with ETA, send an email to sddc.safb.pki@us.army.mil
How do I sync up the certificate with ETA?	Login to ETA using user id and password, At the ETA home page go to "Support" top row of buttons, Register Certificate, Register Certificate link, yes, complete CAPTCHA, Certificate Saved. Log out of ETA, close browser. Login using cert, select the ETA userID you are accessing.
Will TSP Agents accessing DPS need to purchase a digital certificate? (referring to insurance, bond, 3rd party billing, rate filers, or claims companies)	yes, all commercial users are required to purchase one certificate per person.
Will ETA continue to maintain IDs? (today my	yes behind the scenes

digital is linked to a ETA ID)	
Will one digital certificate be allowed access to all TSP accounts (this is a key need to minimize a TSPs cost)	No, this is one cert per person
Can a user have 10, 20, or 30+ digital certificates on one PC?	Yes
Can a digital certificate be loaded on more than one PC and work from both? (when people travel they must now have digital certificates on their laptop)	certs can be loaded on multiple workstations, but can only be accessed by one person.
Will DPS military member be required to be buy a cert?	No, there will be alternatives because it is unlikely that DoD will issue CACs to family members
How do I prove my citizenship?	Indentrust: Within the ECA Program, an Applicant can prove his or her citizenship using a valid passport issued by the country of citizenship. You should bring the passport to the in- person identity verification appointment. Either the Trusted Correspondent, the Notary Public, the U.S. consul or an authorized IdenTrust employee will verify your citizenship using your passport.
Why do I have to prove my citizenship?	Indentrust: Citizenship will be used as part of the criteria for authorizing restricted access by the different Relying Parties to online applications. The ECA Program is governed by a Certificate Policy requiring that all applicants provide proof of their citizenship in order to be issued ECA certificates after July 1st 2007.

How many citizenships can I include in my application?	Indentrust: You can include multiple citizenships in your application. The citizenships you include will be used by IdenTrust to issue your certificate and Relying Parties will use the citizenship information within the certificate to establish your access to applications. IdenTrust has designed its registration processes to easily accept up to three citizenships. If you need to include more than three citizenships please contact the IdenTrust Registration Desk directly at 1-888-882-1104 or 801-924-8141 (from outside the U.S.).
I do not have a passport, what can I do to prove my citizenship?	Indentrust: The ECA program Certificate Policy (CP) and IdenTrust Certification Practice Statement (CPS) require that citizenship be proved based on a valid passport. If you are citizen of a country other than the United States and you do not have a passport, you are not eligible to obtain a certificate under the ECA Program. However, if you are citizen of the United States, you can also prove your citizenship based on the following documents.
	i. Certified birth certificate issued by the city, county, or state of birth, in accordance with applicable local law. A certified birth certificate has a registrar's raised, embossed, impressed or multicolored seal, registrar’s signature, and the date the certificate was filed with the registrar's office, which must be within 1 year of birth. A delayed birth certificate, filed more than one year after birth, is acceptable if it lists the documentation used to create it and is signed by the attending physician or midwife, or lists an affidavit signed by the parents, or shows early public records.
	ii. Naturalization Certificate. A Naturalization Certificate is a document issued by the U.S. Citizenship and Immigration Service (USCIS) since October 1, 1991, and the Federal Courts or certain State Courts on or before September 30, 1991, as proof of a person obtaining U.S. citizenship through naturalization.
	iii. Certificate of Citizenship. A Certificate of Citizenship is a document issued by the U.S. Citizenship and Immigration Service (USCIS) as proof of a person having obtained U.S.

	citizenship through derivation or acquisition at birth (when born outside of the United States).
	iv. FS-240 - Consular Report
	v. DS-1350 - Certification of Report of Birth
What is a Trusted Correspondent?	Indentrust: A Trusted Correspondent is an individual who assists IdenTrust by confirming and documenting the identification of a Subscriber. A Trusted Correspondent may be one of two types: A Trusted Internal Correspondent who is an employee of the same Subscribing Organization as the Subscribers to be identified. A Trusted Internal Correspondent is ordinarily appointed by the Subscribing Organization subject to IdenTrust's approval. The other type of Trusted Correspondent is a Trusted External Correspondent, which is an independent third party under contract directly with IdenTrust and acceptable to the Subscribing Organization. Trusted External Correspondents differ from their internal counterparts in that they are not employees of the Subscribing Organization and are not nominated by it. Instead, Trusted External Correspondents are third parties under contract directly with IdenTrust separate from any Subscribing Organization, although their service availability, location, and convenience factors must be acceptable to the Subscribing Organization and Subscriber for them to provide their services in a given instance.
How do I become a Trusted Correspondent?	Indentrust: When IdenTrust enters into a contract to provide certification services to a Subscribing Organization, that contract obligates the Subscribing Organization to nominate a Trusted Internal Correspondent and cite the nominee’s role in the Subscribing Organization and qualifications as a Trusted Internal Correspondent. The nominee is appointed when IdenTrust accepts the nomination within a time limit specified in the contract. In the event that the nomination is rejected, another one is required. Appointment as Trusted Internal Correspondent includes authorization by the Subscribing Organization to fulfill all responsibilities of a Trusted Internal Correspondent on behalf of the Subscribing Organization as prescribed in the ECA CP

	and the IdenTrust ECA CPS. The Trusted Internal Correspondent accepts the appointment and becomes personally obligated accordingly. The Subscribing Organization is similarly obligated and can bring the Trusted Internal Correspondent under the Organization's employee disciplinary powers, should that be necessary.
How much does it cost to become a Trusted Correspondent?	Indentrust: The only cost for the setup of a Trusted Correspondent is the Medium Hardware Assurance that he or she requires to perform the Trusted Correspondent functions.
Where do I find a Trusted Correspondent?	Indentrust: Your Organization might have a Trusted Correspondent and the person who requested that you obtain an ECA Program certificate will know the contact information for that person. If you do not have the means to obtain this information, contact IdenTrust for further details at 1-888-882-1104. Additionally, IdenTrust has made available Trusted Correspondents in a few cities in the U.S. including: Decatur (AL), Miami (FL), New York (NY), Rockville (VA/MD/DC) and San Francisco (CA). You can contact IdenTrust to set up an appointment.
Can I use a notary to comply with the in-person identity verification requirement?	Indentrust: Yes, you can use a Notary Public to comply with the in-person verification requirement. However, verification by a Notary is valid ONLY for Medium Assurance certificates. If you need to obtain a Medium Hardware Assurance certificate, you must contact a Trusted Correspondent within your organization or an IdenTrust Registrar (RA Operator or Trusted Correspondent).
Can I visit a US consul in-person to comply with the identity verification requirement?	Indentrust: Yes, the ECA Certificate Policy specifies three categories of applicants: U.S. Citizens, citizens of Australia, Canada, New Zealand, or the United Kingdom, and citizens of other countries. U.S. Citizens can appear at any US consulate office for in-person identity verification. Citizens of one of the countries above may visit a US consulate in any of the four countries. If you are not in the U.S and are not a citizen of any of those four countries, you

	should contact a Department of Defense (DOD) country representative for more information. Please be aware that U.S consuls only provide authentication that enables you to obtain a Medium Assurance certificate.
I lost my encryption certificate, how do I get a copy from you?	Indentrust: You need to contact a Key Recovery Officer (KRO) within your organization to initiate a Key Recovery Request. He or she will assist you in filling out the appropriate form. After the form is submitted to IdenTrust and is approved, you will receive a copy of your recovered key in the mail. If your organization does not have a KRO, you can contact specific individuals within your organization who can submit a request on behalf of the organization to IdenTrust. Those individuals are mentioned in the Subscribing Organization Authorization Agreement. Contact your supervisor or your HR department to find out who can request key recoveries from IdenTrust Alternatively, IdenTrust provides KRO services in selected cities including: Decatur (AL), Miami (FL), New York (NY), Rockville (VA/MD/DC) and San Francisco (CA). You can contact IdenTrust to set up an appointment.
I lost my token/smart card, what do I do?	Indentrust: The first step is to revoke your certificate to prevent anyone else from using it. Please be aware that a revoked certificate is unusable. To see what to do for revocation click here: http://www.identrust.com/certificates/eca/eca_revoke.html
	The next step depends on whether you have a backup copy of your encryption private key and if you have received encrypted data or email with it. If you have not used the encryption certificate to receive encrypted data or email, you do not need to recover the encryption key. If you have encrypted data and have no backup copy of your key, see the answer to question 11: How do I get a copy of my encryption certificate?.
	If you need an ECA certificate for your daily functions, you will need to obtain a new certificate.
I need to decrypt a terminated employee's files,	Indentrust: You will need the encryption private key and certificate that was originally used to

what do I do?	encrypt the data. If you do not have a copy of the private key, you can request a key recovery from IdenTrust by using the services of an internal KRO. If your organization does not have a KRO, you can request key recovery directly from IdenTrust if you have the authority to do so. Please review the Subscribing Organization Authorization Agreement to find out who has authority to request key recovery.
I am a law enforcement officer conducting an investigation and need to decrypt a suspect's email, what do I do?	Indentrust: You can request encryption key recovery from IdenTrust. Please contact the organization who originally purchased the certificate or IdenTrust at 1-888-882-1104.
Do you support a browser different from Microsoft's Internet Explorer (IE)?	Indentrust: IdenTrust supports the issuance of Medium Certificates in any browser that can import certificates encapsulated in a PCKS12-type file. For Medium Hardware Certificates, IdenTrust requires you to use browsers that support and have enabled the "ActiveX control" feature. To enable the ActiveX Control feature in Microsoft's Internet Explorer click here
Can I use Mozilla Firefox for my Medium Assurance certificate?	Indentrust: Yes, you can Mozilla FireFox to generate and store a Medium Assurance certificate. However, you are under the obligation to use FireFox under "FIPS mode" in order to properly protect the certificate. See question below entitled "How do I configure Mozilla FireFox to be FIPS 140 compliant?"
How do I configure Mozilla Firefox to be FIPS 140 compliant/validated?	Indentrust: These instructions are provided for Mozilla FireFox version 2.0 or higher. Lower versions follow the same pattern. You can make your Mozilla FireFox browser compliant with FIPS 140 by going to the "Tools" menu, then selecting "Options" and the "Advance" tab. There select the "Encryption" tab and click on "Security Devices." The browser will open a "Device Manager" screen that has an "Enable FIPS" button, click on it and then "OK". The button will change to "Disable FIPS." Your browser is now FIPS compliant. You can now download your ECA certificates.

What is a FIPS112-compliant password?	Indentrust: A FIPS 112-compliant password requires the following characteristics:
	i. Composition: Password should contain both upper and lower case characters (e.g., a-z, A-Z) and have digits and punctuation characters as well as letters. Example: 0-9, !@#$%^&*()_+|~-=\‘,-*+:";’<>?,./)
	ii. Length: The minimum length is 8 characters. Longer passwords will provide stronger security. Passwords are more easily remembered as a passphrase. Example: Don’tUseMyExactExample2
	iii. Lifetime: The maximum life is 1 year and a change is recommended every three months where practical. "Passwords shall be replaced as quickly as possible, but at least within l working day from the time that a compromise of the password is suspected or confirmed"
	iv. Source: Users should not select a password that can be found in a dictionary or name list
	v. Ownership: Passwords should not be shared
	vi. Distribution: Passwords should not be shared in email
	vii. Storage: Passwords should not be stored insecurely
	viii. Entry: Passwords should be entered in a way that others cannot observe entry
	ix. Transmission: Passwords should never be transmitted in clear text
	x. Authentication Period: Users are recommended to lock their screen when leaving their area and to have an inactivity, auto-lock, password-protected screensaver set to protect unauthorized use of their token and system
Should I protect my certificate with a password?	Indentrust: Yes, your certificate is stored along with the private key in your cryptographic module: your browser, your smart card or USB token. According the ECA Certificate Policy and the Subscriber Agreement you accepted, it is your obligation to protect the private key with reasonable security, including a password. The password should be FIPS 112 compliant. See question "What is a FIPS112-compliant password?" for additional information.

What type of certificate should I buy Medium Assurance or Medium Hardware Assurance?	Indentrust: The type of certificate that you require depends on the application you are going access. You should consult with the organization that owns the application for their recommendation on the appropriate assurance level for your certificate.
Does IdenTrust provide identity verification services?	Indentrust: Yes, IdenTrust will offer identity verification (Identification and Authorization - I&A) in selected locations: Decatur (AL), Miami (FL), New York (NY), Rockville (VA/MD/DC) and San Francisco (CA). You can contact IdenTrust to set up an appointment at 1-888-882- 1104.
Which is better, a smart card or a USB token?	Indentrust: IdenTrust has selected smart card and USB devices that are FIPS 140 level 2 that comply with the security requirements outlined in the ECA Certificate Policy. Both devices provide 32Kbytes of memory that exceed your storage needs for ECA certificates. Both devices are comparable and you can use either one without any concerns. To make your final decision, you should consider other factors such as portability and your level of comfort using either technology.
Do you sell component/code signing certificates?	Indentrust: IdenTrust does not sell component or code signing certificates at this time.
What is the "Root Certificate"?	Indentrust: The Root Certificate is the highest level certificate within the ECA Public Key Infrastructure (PKI). This Root Certificate is necessary to enable proper behavior of ECA certificates for validation purposes. IdenTrust always downloads the Root Certificate to your cryptographic device and other intermediate subordinate CAs at the time you retrieve your certificate. However, in a few cases when those certificates are corrupted, you can download them from these locations:
	i. https://crl.gds.disa.mil/
	ii. You can also download the IdenTrust subordinate CA from:

	1. ldap://ldap.identrust.com/cn=IdenTrust ECA[X],ou=Certification Authorities, ou=ECA,o=U.S.Government,c=US?caCertificate;binary
	2. http://apps.identrust.com/roots/identrusteca[X]ca.cer
	Where [X] = Iteration of IdenTrust ECA CA (e.g., ECA1, ECA2, etc.).
	For additional verification, you should contact IdenTrust to verify the fingerprint or serial number in the subordinate CA certificate.
Where do I find The CP? The CPS? The Notary form? The ID form? Key Recovery form? Claim form?	Indentrust: You can find all the forms to do business within the IdenTrust ECA PKI in the following location: https://secure.identrust.com/certificates/policy/eca/
I have incurred losses by using an IdenTrust certificate, who should I complain to?	Indentrust: Please refer to the IdenTrust ECA CPS section 2.4.3. "Dispute Resolution Procedures"
I am a DOD employee/resource, what type of certificate do I need?	Indentrust: You should check with your DOD representative to verify that you need a certificate that is governed by the ECA Certificate Policy. The DOD has internal PKIs not related to the ECA Program.
I need to find my co-worker's certificate, where can I find it?	Indentrust: All IdenTrust ECA certificates are published to a directory that works with the LDAP protocol. You can find any certificate that has been issued by IdenTrust if you:
	i. Open your browser
	ii. Type within the address bar the following: ldap://ldap.identrust.com
	1. The Microsoft Internet Explorer opens a window where you can type in the email address or name of the person whose certificate you are looking up
	2.The Mozilla FireFox asks if you want to launch an external application, click on "Launch application" and then provide the email or name of the person whose certificate you are looking up

	iii. Review under priorities the "Digital IDs" tab and "Export" the appropriate certificate to your computer.
Can I suspend my certificate?	Indentrust: No, the ECA Certificate Policy does not permit suspension.
How do I revoke my certificate?	Indentrust: The process varies depending on who you are. If you are:
	i. The Subscriber and still have access to the certificate, contact IdenTrust's Help Desk HelpDesk@identrust.com, or your Trusted Correspondent, via a signed email requesting the revocation of your certificate. You should also call IdenTrust customer support to confirm the revocation. If you do not have access to the certificate, contact your Trusted Correspondent. After verifying your identity, he or she will submit a request to IdenTrust.
	ii. If you are an Authorized Officer in the Subscribing Organization and are trying to revoke a certificate from someone different than you, submit the request to your internal Trusted Correspondent via a signed email or visit him or her in-person. After identity and authority verification, the Trusted Correspondent will submit the request to IdenTrust. You can also submit the request directly to IdenTrust via a signed email. You should also call IdenTrust customer support to confirm revocation. IdenTrust will verify you are authorized to request revocations on behalf of your organization and continue with the revocation.
How do I Backup/ Export a certificate?	Indentrust:
Internet Explorer 6+	1. Click on 'Tools' menu; on 'Internet Options'; 'Content' tab; 'Certificates' button.
	2. Click once on the certificate you wish to export.
	3. Click the 'Export' button, and click 'Next' on the first screen.
	4. Make sure that "Yes, export the private key" is chosen, then click 'Next'.
	5. Leave the box of "Enable strong protection" checked. Although not necessary, we also recommend putting a check in the "Include all certificates in the certification path if possible"

	box. Click 'Next'.
	6. It will now ask for a new password to be created. Type in any password of your choosing. (and re- type it in the appropriate box). Keep in mind that it is case-sensitive. Any capital letters you use will also need to be used later. Click 'Next'.
	7. Click the 'Browse' button. Choose a drive and folder you would like to store the file. Then type in a name you would like the file to have. Click 'Save'. Click 'Next'.
	Click 'Finish'. If it asks you to click OK, do so. If it is asking for a password, then this would be the same password it asks for when you normally use the certificate online.
	NOTE: the saved file will look like an open envelope with a key in front.
How do I digitally sign or encrypt an email message?	Indentrust: Configure Outlook with a default certificate
	1. In Outlook 2007 go to 'Tools' choose 'TrustCenter' and then 'Email Security'
	2. In the "Encrypted e-mail" section, click the 'Settings' button.
	3. Define the following settings:
	o Security Settings name (This can be named anything you would like)
	o Cryptographic Format = S/MIME
	o Check the box "Default Security Setting for this cryptographic message format"
	o Check the box "Default Security Setting for all cryptographic messages"
	4. Under the "Certificates and Algorithms" section, click on 'Choose'. Next to the "Signing Certificate"
	5. Select the certificate and click 'OK'
	6. (Optional) Under the "Certificates and Algorithms" section, click on 'Choose'. Next to the "Encryption Certificate"
	7. Select the certificate and click 'OK'
	8. After both the Signing and Encryption certificate fields have been populated, click on 'OK' to apply the settings.

	Choose to sign and/ or encrypt individual emails
	Within the email message, click the sign or encrypt button. At the top of the page.
	1. Signing:
	2. Encryption
	Digitally signing an email ensures the recipient that the email has been sent from a specific email address and the message has not been altered. Encrypting emails will prevent anybody from viewing the message besides the recipient with the corresponding certificate.
How do I Backup/ Import a certificate?	Indentrust:
	1. Locate the backup file previously saved/ exported.
	2. Double-click the file. The "Certificate Import Wizard" will open. Click 'Next'.
	3. Click 'Next'.
	4. Type in the password that was chosen when exporting the certificate. The check-boxes on this screen are optional, but we recommend putting checks in both. Here is the description of each:
	a. "Enable Strong Private Key Protection": If this is not chosen, then IE stores your certificate (and private key) with low security. If it is enabled, it will allow you to choose "Medium" or "High" security later. High security causes IE to ask you for a password each time the certificate is used. Medium security causes IE to ask if you're sure each time the certificate is used.
	b. "Mark The Private Key As Exportable": If this is not chosen, then you can never export this certificate from this computer in the future.
	5. The "Certificate Store" window should open. (If you had put the check mark in "Include all certificates..." when exporting previously.) Click 'Next'.
	6. Click 'Finish'.
	7. If "Enable Strong..." in step 4 was chosen, then "Importing a new private exchange key" window opens. By default, it is set to Medium security (as described in step 4a above). If you

	choose to use High security, then click the "Set Security Level" button, and follow the instructions there.
	8. Click 'OK' on the "Importing a new private exchange key" window.
	It should show "The import was successful". Click 'OK'.
How do I replace my digital certificate?	Indentrust: To ensure there is no confusion about replacing a certificate: Replacing your digital certificate is a process where your existing certificate (within the same account with us) is revoked, and a new certificate is created.
	Reasons for replacement:
	This process is normally only needed if your current certificate unusable for some reason.
	1. You have misplaced or forgot your private key password.
	2. The certificate is missing from your computer.
	3. Certificate is not working properly.
	A 'Certificate Replacement' can only be accomplished on certificates where we do not have a copy of an encryption certificate private key. Example types: TrustID, ACES, DOD IECA, SWA Standard-Assurance browser, SWA High/Intermediate Signing-Only.
	For accounts where we do escrow (save a copy of) the encryption private key, a 'Certificate Replacement' is not an option. A 'Key Recovery' needs to be done instead.
	To replace a digital certificate follow these instructions:
	1. Log into our online Certificate Management Center:

	o If it asks you to choose a certificate to log in with, click 'Cancel'.
	o Enter in your account number, and IdenTrust Passphrase. (the passphrase you entered when you first applied for the certificate)
	2. Look for the drop-down box under "Valid Certificates". Select "Replace my certificate", and click the 'Continue' button.
	3. Click 'Next'.
	4. Record your activation code and enter your Passphrase, Click ‘Next’
	5. Keep the default setting and click ‘Next’
	6. Choose a security level and click ‘Next’:
	o High - Requires you to enter a password each time the certificate is used.
	o Medium - Will only prompt you when the certificate is being used.
	7. Click ‘Finish’ then click ‘OK’
	8. Click ‘Next’ then ‘Next’
	9. Click ‘Finish’
	Your certificate is now installed on your computer and ready for use.
How do I get an ECA Identity and Encryption Certificate?	Indentrust: Take a look at the Individual Identity and Encryption Certificate Request Instructions.
I get an error message saying that a “1B6” error has occurred?	Indentrust: This occurs when using Microsoft Internet Explorer on a computer with Microsoft Windows Vista operating system (and sometimes when using Microsoft Internet Explorer 7.x on a computer with Microsoft Windows XP operating system). This error message means that no certificate keys were generated by the Microsoft operating system. This does NOT mean that ORC certificates do not work in Internet Explorer (ORC certificates DO work in Internet Explorer), it means that the Microsoft operating system on your computer will not generate keys. Key generation is the first step in the creation of a digital certificate, but Microsoft is no longer

	supporting common procedures for generating certificate keys
	We recommend that you download and install Mozilla Firefox (available at: http://www.mozilla.org/). Mozilla based web browsers (Netscape and Firefox) have the capability of generating keys on their own; they do not rely on the computer's operation system for this. (FYI – this is why Firefox can generate keys on an Apple Macintosh computer.) You can make your requests and then import the issued certificates via Mozilla Firefox. You then make back-up files of the certificates (something you want to do regardless of what browser you use) and import the certificates into Internet Explorer.
Why am I getting a Security Alert message that there is a problem with the ORC site's certificate?	Indentrust: You have not properly trusted the ORC ECA Certificate Authority.
	Go to the ORC ECA Instructions page and find the instructions for your browser to Trust the ORC ECA Certificate Authority
I am being asked for a password but haven't created one yet.	Indentrust: This should only occur if you are using Netscape or Firefox. These browsers use something called a "Master Password" to protect the certificate store (also called the software security device and the internal cryptographic device). This Master Password also protects the "Password Manager" function in these browsers. So, if you are using the Password Manager feature, you may have set the Master Password at some previous time. If you can not recall (or can not discover) the correct Master Password, then you should 'reset' the Master Password BEFORE you make and submit certificate requests.
	WARNING: If you reset the Master Password, all information protected by that Master Password (the Password Manager and the certificate store) will be deleted. So this will destroy any certificates currently protected by the Master Password that you are resetting.
Can I get certificates on my Apple Macintosh computer?	Indentrust: Yes, but not we do not recommend that you use Safari; you should install a different browser.

	We recommend that you download and install Mozilla Firefox (available at: http://www.mozilla.org/). Mozilla based web browsers (Netscape and Firefox) have the capability of generating keys on their own; they do not rely on the computer's operation system for this. You might want to consider downloading/installing Thunderbird (the email client companion to Firefox) if you need to use digitally signed/encrypted email.
I get an error message that the CA cannot process my request.	Indentrust: The CA requires specific syntax for certificate requests. Most of this syntax is generated or checked by the form. However, in some cases, the input form allows incorrect syntax. Request the certificate again and make sure that all fields are filled in, and that there are no commas in the entries. It is better to start from https://eca.orc.com and click the request a certificate instead of using the back button because sometimes the browser does not correctly resubmit data from the form.
	Accepting a Certificate
I am copying the URL from the email message, but I keep getting an error message.	Indentrust:
	The URL should like:
	"https://server .eca.orc.com/cms?op=displayBySerial&serialNumber=xx"
	or
	"https://server .eca.orc.com/cms?op=displayBySerial&serialNumber=xx:xx"
	where server is the name of the CA that the certificate was requested from, and the xËs are hexadecimal numbers. Generally, the problem is that the end of this URL is chopped off. Have the subscriber key the end of the URL into their browser.
When I try to download my issued certificate, I get an "Accept in PKCS7" error message.	Indentrust: If you are getting the "Error in accept PKCS7" message that means that the Microsoft OS/Internet Explorer can not find the private key(s) for those certificates. (Please note that this does not necessarily mean that the private key(s) are not there, just that the MS system can not

	find them.)
	This happens because:
	the request was done under a different log-in profile (you are logged on under a different username/password) than when the request was made
	or the request was made with a different browser (for example, Firefox)
	or the request was made on a different computer than the one you are trying to import it on
	or something was done to the machine (like an update to the operating system - a Windows update, profile change, computer re-imaged, etc.)
	You will only be able to import the issued certificate onto the same computer, same log-in profile, and using the same web browser as when you made the on-line request. (i.e. as when you got the “Print this form” web page).
I get the error message that there is no matching private key.	Indentrust: This is the Mozilla (Netscape/Firefox) equivalent to the Microsoft “Accept in PKCS7” error message discussed above.
	This happens because:
	the request was done under a different log-in profile (you are logged on under a different username/password) than when the request was made
	or the request was made with a different browser (for example, Internet Explorer)
	or the request was made on a different computer than the one you are trying to import it on
	or something was done to the machine (like an update to the operating system - a Windows update, profile change, computer re-imaged, etc.)
	You will only be able to import the issued certificate onto the same computer, same log-in profile, and using the same web browser as when you made the on-line request. (i.e. as when you got the ?Print this form? web page).
I am using a different workstation.	Indentrust: If you have switched workstations, or are trying to accept the certificate from home,

	you will be unable to retrieve the certificate. Go back to the original workstation that was used to request the certificate. Once the certificate has been accepted, it can be exported and imported into other workstations.
My workstation has been upgraded since the request was made.	Indentrust: If your workstation has been upgraded (ie new operating system or new version of Netscape), the private key that goes with the certificate may have been inadvertently deleted. If so, it cannot be recovered. You will have to delete the certificate database file, request a new certificate, and request that the current certificate be revoked.
My password is not working.	Indentrust: Passwords are case sensitive.
	If the subscriber cannot remember his or her password, it cannot be recovered. He or she will have to request a new certificate, and request that the current certificate be revoked. (See password issues and tips.)
How do I take my certificate to a new workstation?	Indentrust: You can export your certificate to a floppy disk and import it on another workstation. See the subscriber instructions for exporting and importing certificates.
I have a certificate, but I cannot access the application.	Indentrust: If a certificate is rejected from the application, either the application requires additional access approval beyond holding an ECA PKI certificate, or the certificate is not properly loaded into the directory that the application is using. Check the directory listing directly. If the certificate is not there, contact ORC for assistance. If the certificate is there, contact the application technical support for assistance.
Should I purchase a certificate now or wait till closer to October?	It is up to the user when to purchase the certificate. Keep in mind, the certificate will expire in one year. PKI program office recommends purchase before 1 Oct 2011 deadline to insure certificate is operational.
If I purchase the certificate now do I continue to	Once a certificate is purchased and synced with ETA, user can no longer use user id/password.

access the SDDC with my user name and password until October 1st?	
Some of our competitors are retired military but have been allowed permission to use a "us.army.mil" email address and this allows them access to SDDC and other DOD sites that we can not access. SDDC will have to require those retired former military personnel to cease and desist this practice as it provides them with a competitive advantage to information that a non-"us.army.mil" has access to and now at a further reduced cost	Retirees do not retain a CAC with a certificate. Users that use .mil email address have been required to use a certificate since the summer of 2010.
Are we able to access the ETA website until we acquire a digital certificate?	That is correct. ETA will not be completely certificate accessible until 1 October 2011. We recommend the purchase of the certificate before the deadline to insure operational access.
Are instructions available for this transition?	ETA help page provides FAQ's, where to purchase the cert, and how to sync the cert with ETA upon receipt.
Could you please tell me where to get a reader	Do a Google search on CAC reader and a list of where to purchase and a price comparison can be found.
What type of certificate should I buy?	Medium assurance
IdenTrust website and instructions require the following information: - Organization's Full Name and Headquarters Address - Dun & Bradstreet D-U-N-S Number (optional)	PKI Team called their support line to question the need for company information. The direction provided was that it is a requirement of IdenTrust to have a company association and that an individual could not obtain an ECA without one.
Will I have to have more than one certificate per SCAC?	No.

Will we be allowed for another exemption using ECA or will that option no longer be available?	At this time, there are no exemptions for commercial transportation providers.